St. John's Law Review

Volume 93
Number 2 *Volume 93, 2019, Number 2*

Article 6

January 2020

The (Possibly) Injured Consumer: Standing in Data Breach Litigation

Lauren M. Lozada

NOTES

THE (POSSIBLY) INJURED CONSUMER: STANDING IN DATA BREACH LITIGATION

LAUREN M. LOZADA[†]

INTRODUCTION

Equifax, Deloitte, Yahoo, Pizza Hut, Uber, FedEx, MyFitnessPal, Reddit, T-Mobile, British Airways, Facebook, Google+, and now Marriott Hotels. Other than being household names, what do these companies have in common? Within the last three years, all have suffered significant data breaches,[1] leaving their consumers vulnerable to identity theft. According to an ongoing study, 944 breach incidents occurred in the first half of 2018 alone.[2] These breaches compromised a total of 3,533,172,708 consumer data records—over eighteen million records every day.[3] "Today's organizations face a cybersecurity landscape more difficult to navigate than ever before. As our world grows more interconnected and technology-dependent, cybercriminals are becoming more sophisticated in their attacks and are keeping pace with our efforts to thwart them."[4] These frequent attacks raise an important question—what are consumers to do after a breach has occurred, and should the breached companies be forced to bear the consequences of hackers' actions?

[†] Associate Managing Editor, *St. John's Law Review*, J.D. Candidate, 2020, St. John's University School of Law; B.S., Hofstra University, 2010.

[1] *The Most Infamous Data Breaches*, TECHWORLD (Apr. 16, 2019), https://www.techworld. com/security/uks-most-infamous-data-breaches-3604586/.

[2] *Data Privacy and New Regulations Take Center Stage, Breach Level Index: 2018 First Half Review*, GEMALTO 2 (Oct. 16, 2018), https://breachlevelindex.com/request-report [hereinafter *Breach Level Index*].

[3] *Id.* at 2. This represents a 72% increase over the same period in 2017. *Id.* at 4.

[4] *Data Breach Industry Forecast 2018*, EXPERIAN DATA BREACH RESOLUTION 2, http://www.experian.com/assets/data-breach/white-papers/2018-experian-data-breach-industry-forecast.pdf (last visited June 24, 2019).

Many consumers, unable to determine hackers' identities, seek instead to bring legal action against the companies that failed to safeguard their data. For the consumer who has experienced some form of identity theft—for example, fraudulent charges on her accounts or unauthorized accounts created in her name—the path to the courtroom is relatively straightforward. For those whose data has not (yet) been misused, however, the requirement of constitutional standing presents a significant obstacle. Article III of the United States Constitution limits judicial power to the adjudication of "[c]ases" or "[c]ontroversies" between parties.[5] Under current case law, in order to successfully establish standing, a plaintiff must allege:

> (1) it has suffered an "injury-in-fact" that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.[6]

In the context of a data breach where no actual, concrete injury has yet occurred—that is, identity theft—the question becomes whether any future harm is in fact "imminent." In the midst of an existing circuit split on what qualifies as "imminent," the United States Supreme Court in its 2013 *Clapper v. Amnesty Int'l USA* decision explained that a sufficiently "imminent" injury is one that is "certainly impending" or, at a minimum, poses a "substantial risk" of future harm.[7] This explanation,[8] however, did little to reconcile the circuit split, and inconsistent results in such cases have continued.

This Note will address the question of what factors a prospective plaintiff must display to "push [a] threatened injury of future identity theft beyond the speculative to the sufficiently imminent."[9] Part I will delve into relevant statistics to identify the characteristics of a data breach that most often lead to eventual identity theft. Part II will explore recent data breach standing cases and analyze the factual differences and legal

---

[5] U.S. CONST. art. III, § 2 cl. 1.

[6] Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180–81 (2000) (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992)).

[7] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409, 414 n.5 (2013).

[8] Notably, the *Clapper* decision was unrelated to consumer data breaches, *see id.* at 401, and the Supreme Court has yet to decide a standing case in this particular context.

[9] Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017).

perspectives that have led to disparate results among the federal circuits. Lastly, Part III will recommend a method for evaluating future data breach standing issues.

I. BACKGROUND ON DATA BREACHES

The Identity Theft Resource Center ("ITRC") defines a data breach as "an incident in which an individual name plus a Social Security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure."[10] Since 2005, the company has been tracking security breaches in order to identify patterns and trends that could help consumers and businesses better protect personal identifying information.[11] Much of the ITRC's methodology and findings center around one concept: "data breaches are not all alike."[12] When attempting to determine the magnitude and likelihood of the potential harm associated with a breach, several factors should be taken into account: (1) the source of the breach; (2) the type(s) of data compromised; and (3) the industry in which the breached company operates.[13]

A. Breaches by Source

Because the ITRC recognizes method of exposure as a "critical category" in evaluating the future harm stemming from a breach, it divides cyberattacks into seven categories: "hacking (with subcategories of phishing, ransomware/malware, and skimming), unauthorized access,[14] insider theft, data on the move, accidental exposure, employee error/negligence/improper disposal/loss, and physical theft."[15] Since 2011, hacking has been the most common type of attack, increasing annually from approximately 25–30% of the total breaches in 2011 to an overwhelming 59.4% in 2017.[16]

---

[10] *2017 Annual Data Breach Year-End Review*, IDENTITY THEFT RESOURCE CENTER 19 (Jan. 18, 2018), https://www.idtheftcenter.org/2017-data-breaches/ [hereinafter *ITRC Data Breach Report*].

[11] *Id.*

[12] *Id.*

[13] *See id.* at 19–20; *see also Breach Level Index*, *supra* note 2, at 6–11.

[14] The ITRC defines unauthorized access as "breaches which involve some kind of access to the data but the publicly available breach notification letters do not explicitly include the term hacking." *ITRC Data Breach Report*, *supra* note 10, at 4.

[15] *Id.*

[16] *Id.*

Cybersecurity company Gemalto's *Breach Level Index* employs a similar methodology, dividing breaches into the categories of malicious outsider, accidental loss, malicious insider, hacktivist,[17] and unknown.[18] Malicious outsider—arguably the most analogous to the ITRC's hacking category—again consistently represents the most prevalent type of breach.[19] Of the 3.35 billion records reportedly compromised in the first half of 2018, nearly 2.5 billion, or 73%, were the result of attacks by malicious outsiders.[20] Accidental loss, encompassing mistakes and misconfigurations, was the second most prevalent source of breaches in the first half of 2018, accounting for 34% of breach incidents and 26%—nearly 880 million—of total compromised records.[21] Notably, the number of records compromised by accidental loss was cut nearly in half compared to the same period in 2017.[22] Whether this reduction was by chance or due to a concerted effort by companies to better safeguard consumers' data remains to be determined.

In response to the ever-increasing frequency of data breaches, Congress has considered enacting national legislation that would require companies to notify affected individuals of a breach.[23] To that end, Congress tasked the Government Accountability Office ("GAO") with evaluating the extent to

---

[17] Oxford Dictionaries defines the term "hacktivist" as "[a] person who gains unauthorized access to computer files or networks in order to further social or political ends." *Hacktivist*, ENGLISH OXFORD LIVING DICTIONARIES, https://en.oxforddictionaries.com/definition/hacktivist (last visited June 24, 2019).

[18] *Breach Level Index*, *supra* note 2, at 6.

[19] *Id.* at 7. According to the *Breach Level Index*, malicious outsider breaches accounted for 56% of the total breach incidents in the first half of 2018. *Id.*

[20] *Id.* at 6.

[21] *Id.*

[22] *Id.*

[23] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO 07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (2007) [hereinafter GAO REPORT]. Most states have already enacted breach notification laws, but due to the variability among state statutes, companies that possess data from consumers in multiple states have been forced to invest time and money into developing custom notification schemes, or to adhere to the strictest of the applicable state laws. Brandon Faulkner, Note, *Hacking Into Data Breach Notification Laws*, 59 FLA. L. REV. 1097, 1105, 1110 (2007). For more information on the various state breach notification laws, including an interactive map, see *Summary of U.S. State Data Breach Notification Statutes*, DAVIS WRIGHT TREMAINE LLP, https://www.dwt.com/gcp/state-data-breach-statutes (last visited June 24, 2019).

which data breaches have resulted in identity theft.[24] A summary of the GAO's findings is as follows:

> The extent to which data breaches result in identity theft is not well known, in large part because it can be difficult to determine the source of the data used to commit identity theft. Although we identified several cases where breaches reportedly have resulted in identity theft—that is, account fraud or unauthorized creation of new accounts—available data and interviews with researchers, law enforcement officials, and industry representatives indicated that most breaches have not resulted in detected incidents of identity theft.[25]

The GAO did recognize, however, that the potential harm stemming from a breach is largely dependent on its circumstances, including how the data was compromised.[26] "[B]reaches that are the result of intentional acts," it explained, "[are generally] considered to pose more risk than accidental breaches."[27] Of the twenty-four breaches examined by the GAO,[28] four resulted in known cases of identity theft.[29] All four of these breaches were from intentional acts; three involved hacking, leading to account fraud, and one involved using deception or misrepresentation to obtain personal data, leading to the unauthorized creation of new accounts.[30] Notably, the theft of a

---

[24] *GAO Report, supra* note 23, at 3. The stated objectives of the report were to examine: "(1) what is known about the incidence and circumstances of breaches of sensitive personal information; (2) what information exists on the extent to which breaches of sensitive personal information have resulted in identity theft; and (3) the potential benefits, costs, and challenges associated with breach notification requirements." *Id.*

[25] *Id.* at 5.

[26] *Id.* at 6.

[27] *Id.*

[28] The GAO analyzed lists of breaches maintained by Identity Theft Resource Center, Privacy Rights Clearinghouse, and Congressional Research Service to identify the twenty-four largest data breaches reported in the news media from January 2000 to June 2005. *Id.* at 24, 26. The authors of the report acknowledge that breaches involving criminal activity may consequently be overrepresented, "as such breaches are probably more likely than accidental losses to be reported to authorities and by the news media." *Id.* at 20.

[29] *Id.* at 24. "The term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name." *Id.* at 2.

[30] GAO REPORT, *supra* note 23, at 26.

laptop containing personal information presents a grey area with respect to intent, as it may be unclear whether the laptop was stolen for the hardware, the personal data, or both.[31]

B. Breaches by Type of Data Compromised

The GAO further determined that "[t]he type of data compromised in a breach can effectively determine the potential harm that can result."[32] It explained that "[d]epending on the type of information compromised and how it is misused, identity theft victims can face a range of potential harm, from the inconvenience of having a credit card reissued to substantial financial losses and damaged credit ratings."[33] This is assuming, of course, that unauthorized individuals obtain the information in a usable, or unencrypted, format.[34]

According to law enforcement officials, the ease with which credit and debit card numbers can be misused makes fraudulent charges on existing accounts the most prevalent type of harm resulting from a breach.[35] The ITRC reported that in 2017, credit and debit card information was involved in nearly 20% of breach incidents, impacting over 14 million data records.[36] This represents an increase of 88% compared to the number of records reported in 2016.[37]

While breaches compromising credit and debit card information pose a significant problem, the resulting harm is somewhat mitigated by the existence of laws limiting consumer liability in the event of fraud. By federal statute, consumer liability for unauthorized credit card charges is capped at a

---

[31] *Id.* at 31.

[32] *Id.* at 30.

[33] *Id.* at 2*; see also* Allison Grace Johansen, *7 Steps to Take Right After a Data Breach*, LIFELOCK, https://www.lifelock.com/learn-data-breaches-steps-to-take-right-after-a-data-breach.html (last visited June 24, 2019) ("While stolen credit cards and the like can be canceled and replaced, it's quite difficult to obtain a new Social Security number. And fraudsters can do a lot more with your SSN . . . and other unique, sensitive PII than they can accomplish with an email or credit card account.").

[34] *ITRC Data Breach Report*, *supra* note 10, at 19; *see also* GAO REPORT, *supra* note 23, at 31 (defining encryption as "encoding data so that it can only be read by authorized individuals," and explaining that "encryption does not necessarily preclude fraudulent use of data—for example, if the key used to unencrypt the data is also compromised.").

[35] GAO REPORT, *supra* note 23, at 22.

[36] *ITRC Data Breach Report*, *supra* note 10, at 11.

[37] *Id.* at 4–5.

maximum of fifty dollars per account.[38] Similarly, the Electronic Fund Transfer Act limits consumer liability for unauthorized debit card transactions, depending on how quickly the loss or theft of the card is reported.[39] Some credit and debit card issuers even go so far as to adopt a policy to reimburse all fraudulent charges incurred on users' accounts.[40] Consumers are then left with the relatively minor inconveniences of cancelling and reactivating cards, losing temporary access to account funds, and redirecting automatic payments and deposits.[41]

The unauthorized creation of new accounts, by contrast, may result in severe, long-term financial and other hardships.[42] Depending on the type of data obtained, an identity can be used, among other things, to open bank or credit card accounts, file tax returns, originate home mortgages, or apply for government benefits.[43] Because the unauthorized creation of new accounts generally requires the use of one or more forms of personally identifiable information[44]—typically including social security numbers—it is more difficult and labor intensive to achieve than fraud on existing accounts.[45] Consequently, it is believed to occur much less frequently from data breaches.[46] In fact, officials at the Secret Service, FBI, and USPIS[47] agree that the data needed

---

[38] GAO REPORT, *supra* note 23, at 30 n.47 (citing 15 U.S.C. § 1643 (2012)).

[39] *Id.* (citing 15 U.S.C. § 1693g (2012)).

[40] *Id.* at 30.

[41] *Id.* at 30 n.47.

[42] *Id.* at 30.

[43] *Id.*; *see also* Alison Grace Johansen, *5 Kinds of ID Theft Using a Social Security Number*, LIFELOCK, https://www.lifelock.com/learn-identity-theft-resources-kinds-of-id-theft-using-social-security-number.html (last visited June 24, 2019) (indicating that data thieves can potentially use social security numbers to effectuate financial identity theft, government identity theft, criminal identity theft—essentially using another's identity as a "get out of jail free" card—medical identity theft, and utility fraud).

[44] The GAO Report defines "personally identifiable information" as "any information that can be used to distinguish or trace an individual's identity—such as name, Social Security number, driver's license number, and mother's maiden name—because such information generally may be used to establish new accounts . . . ." GAO REPORT, *supra* note 23, at 2 n.2. Notably, the definition does not extend to "other 'means of identification,' as defined in 18 U.S.C. § 1028(7), including account information such as credit or debit card numbers." *Id.* (quoting 18 U.S.C. § 1028(d)(7) (2012)).

[45] *Id.* at 22.

[46] *Id.*

[47] The USPIS is a division of the U.S. Postal Service responsible for investigating postal-related crimes such as mail fraud, external mail theft, and fraudulent changes of address. *Id.* at 12–13.

to create such new accounts is more often obtained through other means, such as sifting through household trash, than from data breaches.[48]

The ITRC has found that social security numbers, used by many institutions as primary authenticators, are compromised in breaches even more often than credit or debit card numbers.[49] In 2017, more than half of the total reported incidents included social security numbers—an astonishing 158 million records exposed.[50] Still, "[w]hile a Social Security number continues to be the most valuable piece of information in the hands of a thief, even the exposure of emails, passwords or user names can be problematic as this information often plays a role in hacking and phishing attacks."[51]

C. Breaches by Industry

Because different industries deal primarily with certain types and quantities of data, some industries will be more heavily impacted by data breaches than others.[52] For example, retail stores are known to handle a large volume of credit and debit card numbers and are thus particularly attractive targets for a breach.[53] The ITRC found that the business sector—encompassing such entities as retail services, utilities, payment processors, and hospitality—experienced 55% of the total breach incidents in 2017.[54] Breaches in this sector were more impactful than those in other sectors, making up 99% of the total records compromised.[55]

This represents about 188,000 records compromised per breach, as compared to an average of about 22,000 per breach for all other industries.[56] Hacking was the cause of nearly 40% of

---

[48] *Id.* at 22.

[49] *ITRC Data Breach Report*, *supra* note 10, at 4–5.

[50] *Id.* at 5.

[51] *Id.* (quoting Karen Barney, ITRC Director of Program Support).

[52] *See* GAO REPORT, *supra* note 23, at 20.

[53] *See id.*

[54] *ITRC Data Breach Report*, *supra* note 10, at 6, 20. A more complete list of entities in the business category includes "retail services, hospitality and tourism, professional, trade, transportation, utilities, payment processors and other entities not included in the other four sectors. It also includes nonprofit organizations, industry associations, non-government social service providers, as well as life insurance companies and insurance brokers (non-medical)." *Id.* at 20.

[55] *Id.* at 6.

[56] *See id.*, as calculated from the data presented.

Business sector breaches.[57] The second most impacted industry was the "Medical/Healthcare" sector, making up approximately 24% of breaches.[58] The remaining 21% of breaches were divided between the "Banking/Credit/Financial," "Government/Military," and Education sectors.[59]

D. Statistical Challenges

As its title suggests, the GAO's report acknowledges that we do not yet understand the full extent to which data breaches result in identity theft.[60] Although the report was published in 2007, the same challenges still exist in determining the link between data breaches and eventual misuse. Many victims of identity theft have no knowledge of how their personal information was compromised and, as a result, may misattribute suspicious activity on their accounts or credit report.[61] For example, a consumer who has previously been notified of a breach may incorrectly assume that the breach was the cause of a recent fraudulent charge.[62] Moreover, once a consumer's data has been compromised, there is no telling how long after the breach a malicious party may choose to misuse his or her data.[63] "[S]tudies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[64] Lastly, issues of privacy and confidentiality can impede the collection of meaningful data from both breached companies and injured consumers.[65] The implementation of data protection regulations, however, has already led to an increase in the number of reported breaches.[66] With more information available to evaluate the risk associated with particular types of breaches, it may become possible to predict which breaches are most likely to result in eventual identity theft.

---

[57] *Id.* at 4.
[58] *Id.* at 6.
[59] *Id.*
[60] *GAO Report*, *supra* note 23, at 5.
[61] *Id.* at 28.
[62] *Id.*
[63] *Id.* at 29.
[64] *Id.*
[65] *Id.*
[66] *Breach Level Index*, *supra* note 2, at 3; *see also ITRC Data Breach Report*, *supra* note 10, at 3 (quoting Eva Velasquez, President and CEO of the ITRC) ("We've seen the number of identified breaches increase as a result of industries moving toward more transparency, . . .").

II. CASE LAW

A. The "Certainly Impending" and "Substantial Risk" Standards of Review

In *Clapper v. Amnesty Int'l USA*, the Supreme Court was tasked with determining whether an alleged future injury was sufficiently imminent to confer standing. The case was brought by a group of individuals whose professions required them to "engage in sensitive and sometimes privileged telephone and email communications" with others located abroad.[67] They sought to challenge a federal statute that permitted government surveillance of foreign citizens because, in their belief, "there [was] an objectively reasonable likelihood that their communications [would] be acquired under [the statute] at some point in the future."[68] Because the plaintiffs failed to allege that any of their communications had yet been monitored, the Supreme Court denied standing.[69] Alluding to several of its prior standing decisions, the court explained:

> "Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes—that the injury is *certainly* impending . . . ." Thus, we have repeatedly reiterated that "threatened injury must be *certainly impending* to constitute injury in fact," and that "allegations of *possible* future injury" are not sufficient.[70]

The Court also discussed the "highly attenuated chain of possibilities"[71] that would need to occur before plaintiffs would be surveilled, including the government's decision to monitor specific communications, the Foreign Intelligence Surveillance Court's approval to target the plaintiffs' foreign contacts, and finally, the plaintiffs' own participation in the intercepted communications.[72] The Court explained that it "decline[d] to abandon [its] usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors."[73]

---

[67] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 406 (2013).

[68] *Id.* at 407.

[69] *Id.* at 410–11.

[70] *Id.* at 409 (internal citations and alterations omitted) (first quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 564 n.2 (1992); then quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

[71] *Id.* at 410.

[72] *Id.*

[73] *Id.* at 414.

The Supreme Court did, however, leave room for a more forgiving standard to be applied. The Court explained in footnote 5 of the decision:

> Our cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a "substantial risk" that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.[74]

It remains unclear whether the Supreme Court intended for the substantial risk analysis to apply in the particular context of consumer data breach actions. This has led to inconsistency in the standard applied, and to divergent views among circuit courts as to what exactly a plaintiff must demonstrate at the pleadings stage to establish standing.

B. Factors to Consider in Weighing the Imminence of Future Harm

While no bright-line rule exists for determining whether a consumer plaintiff has sufficiently established standing in a data breach action, a small set of common factual details have permeated circuit courts' analyses in recent cases. These factors include: (1) the presence or absence of actual misuse of consumer data as a result of the breach; (2) the type of data compromised in the breach; (3) offers by breached companies to provide free credit monitoring services to effected consumers; and (4) mitigation costs expended by the plaintiff consumer(s).[75] Though frequently taken into account, these factors have not always been interpreted consistently by the courts.

1. Prior Misuse

At its most basic, the concept of prior misuse of consumer data would concern only the plaintiffs named in the particular action. If a plaintiff experienced misuse, the court would confer standing; if not, the court would deny it. When the focus shifts to evaluating the imminence of future harm, however, prior misuse can play another role in the analysis. Any prior misuse of data stolen in the subject breach, whether belonging to a named

---

[74] *Id.* at 414 n.5 (quoting Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 180 (2010) (Stevens, J. dissenting)).

[75] *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 274–77 (collecting cases).

plaintiff or not, speaks to the intent of the hackers in possession of the consumers' data.[76] Even one instance of a hacker making a fraudulent charge or attempting to open an unauthorized account shows that he or she has the requisite scienter to commit fraud. It also shows that the hackers were successful in acquiring enough of the right types of personal data to be able to steal consumers' identities.[77] Both of these inferences lead to an increased likelihood that additional consumers will experience future misuse and may justify consumers in seeking recovery for any preventative measures that they undertake. On the other end of the spectrum, if a breach cannot be shown to have resulted in any instances of attempted identity theft at all, it is not unreasonable to infer that consumers may never experience misuse of their data.[78]

The Ninth Circuit's decision in *In re Zappos.com, Inc.* aptly illustrates this point. Popular retailer Zappos.com fell victim to a breach of its servers, compromising the personal data of more than 24 million customers.[79] In the class action suit that followed, predicated on an increased risk of identity theft, the district court divided the plaintiffs into two groups—(1) those who had suffered harm from actual misuse, and (2) those who had not.[80] The court found that this distinction was dispositive, conferring standing on Group 1, but denying it from Group 2.[81] The plaintiffs in Group 2 then appealed the dismissal of their claims.[82] The Ninth Circuit reversed, finding standing for all plaintiffs.[83] In so holding, the court recognized that, while the plaintiffs whose data had been misused were not part of the

---

[76] *See id.* at 274 (discussing and ultimately distinguishing from cases in which alleged misuse of plaintiffs' personal information indicated that the thief "intentionally targeted" the breached data).

[77] *See* discussion *supra* Part I.B.

[78] *See Beck*, 848 F.3d at 275 (" '[A]s the breaches fade further into the past,' the Plaintiffs' threatened injuries become more and more speculative.") (quoting Chambliss v. Carefirst, Inc., 189 F. Supp. 3d 564, 570 (D. Md. 2016)); *see also* In re Zappos.com, Inc., 108 F. Supp. 3d 949, 958 (D. Nev. 2015) ("[T]he passage of time without a single report from Plaintiffs that they in fact suffered the harm they fear must mean something.").

[79] In re Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018).

[80] *Id.* at 1024.

[81] *Id.*

[82] *Id.*

[83] *Id.* at 1027. Much of the court's discussion concerned whether its earlier decision in *Krottner* remained good law in light of the Supreme Court's subsequent *Clapper* decision. *Id.* at 1025–26. It concluded that "*Krottner* is not clearly irreconcilable with *Clapper* and thus remains binding." *Id.* at 1026, 1026 n.6.

appeal, "their alleged harm undermine[d] Zappos's assertion that the data stolen in the breach [could not] be used for fraud or identity theft."[84]

Similarly, in *Remijas v. Neiman Marcus Group, LLC*, the Seventh Circuit found standing where prior misuse had occurred.[85] Hackers had used malware to infiltrate the computer systems of luxury department store Neiman Marcus.[86] Of the approximately 350,000 credit card numbers compromised in the cyberattack, 9,200 credit cards "were known to have been used fraudulently" after the breach.[87] The customers sought to recover from Neiman Marcus under such theories as negligence and breach of implied contract.[88] They alleged, among other things, "two imminent injuries: an increased risk of future fraudulent charges and greater susceptibility to identity theft."[89] In conferring standing on all plaintiffs in the class action suit, the court reasoned that the plaintiffs' risk of harm was substantial given that "[p]resumably, the purpose of [a] hack is, sooner or later, to make fraudulent charges or assume . . . consumers' identities."[90] "Why else," the court asked, "would hackers break into a store's database and steal consumers' private information?"[91] It is not difficult to see why the court presumed

---

[84] *Id.* at 1027.

[85] 794 F.3d 688, 688–90, 697 (7th Cir. 2015).

[86] *Id.* at 689.

[87] *Id.* at 690.

[88] *Id.* at 690. The complaint also alleged unjust enrichment, unfair and deceptive business practices, invasion of privacy, and violation of multiple state data breach laws based on an array of injuries classified by the plaintiffs as either "actual" or "imminent." *Id.* at 690–92.

[89] *Id.* at 692. In addition to those noted above, plaintiffs claimed to have suffered the "actual" injuries of:

> 1) lost time and money resolving the fraudulent charges, 2) lost time and money protecting themselves against future identity theft, 3) the financial loss of buying items at Neiman Marcus that they would not have purchased had they known of the store's careless approach to cybersecurity, and 4) lost control over the value of their personal information.

Id. With respect to the first two injuries, while recognizing that "[m]itigation expenses do not qualify as actual injuries where the harm is not imminent," the court held that the harm here was imminent, and so the mitigation costs were sufficient to confer standing. *Id.* at 694 (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 417 (2013)). The court, however, expressed doubt as to the last two "actual" injuries, noting "[w]e need not decide whether they would have sufficed for standing on their own, but we are dubious." *Id.*

[90] *Id.* at 693.

[91] *Id.*

that the hackers were acting with malicious intent, in light of their prior misuse of thousands of consumers' credit card information.

In contrast, courts have declined to confer standing where no evidence exists to suggest that hackers intend to misuse consumers' data. For example, in *Katz v. Pershing, LLC*, the plaintiff alleged that her personal data might conceivably be misused someday because it was inadequately protected.[92] Katz did not, however, point to any instance of a breach, let alone actual misuse of her personal data.[93] Consequently, the First Circuit found that "[s]uch a purely theoretical possibility simply d[id] not rise to the level of a reasonably impending threat."[94]

Likewise, in *Reilly v. Ceridian Corp.*, there was no evidence that the hacker so much as "read, copied, or understood" the information in the system.[95] Plaintiffs alleged that their risk of future identity theft had been increased, but the Third Circuit determined that the plaintiffs lacked standing because their allegation of future identity theft rested on an attenuated chain of assumptions and was not certainly impending.[96] In so holding, the court cited to one of its earlier decisions, reasoning that "one cannot describe how the [plaintiffs] will be injured without beginning the explanation with the word 'if.' "[97] Given the absence of any actual or attempted misuse, or evidence that the intrusion into the payroll system was "intentional or malicious," there was nothing to suggest that the data had—or ever would be—misused.[98]

Lastly, in *Beck v. McDonald*, the Fourth Circuit concluded that the plaintiffs lacked standing because they failed to show any evidence that personal information had been accessed or

---

[92] 672 F.3d 64, 70 (1st Cir. 2012). This case arose when the named plaintiff, a brokerage accountholder, alleged that her nonpublic information was vulnerable to prying eyes because her information was inadequately protected by the defendant's services. *Id.* Despite the fact that no known breaches had occurred, Katz purchased identity theft insurance and credit monitoring services to guard against the possibility that her personal information might someday be hacked. *Id.* at 79.

[93] *Id.* at 79.

[94] *Id.*

[95] 664 F.3d 38, 40 (3d Cir. 2011). The case involved a data breach by a hacker who had penetrated a firewall in the defendant's payroll system.

[96] *Id.* at 42.

[97] *Id.* at 43 (alteration in original) (quoting Storino v. Borough of Point Pleasant Beach, 322 F.3d 293, 297–98 (3d Cir. 2003)).

[98] *Id.* at 43–44.

misused by a thief who intended to steal that information.[99] Following the Third Circuit's *Reilly* decision, the *Beck* court reasoned that a conclusion of "certainly impending" identity theft would rest on the attenuated sequence of assumptions that the thieves had stolen the items with the intent to access personal information, that they would then specifically select the named plaintiffs' information from among thousands of others, and finally that they would succeed in an attempt at identity theft.[100] Without evidence to support these assumptions, the theft of the items presented a merely speculative risk of future harm.[101]

2. Type of Data Compromised

As described in Part I.B above, the type of data compromised in a breach weighs heavily on the potential harm that can result. While rarely discussed at length in court opinions, the outcomes of consumer data breach actions likewise appear to be correlated to the type of data involved in the particular breach.[102] When full, unencrypted social security numbers or credit card numbers—data known to be the most useful to identity thieves—were alleged to have been stolen, courts have recognized the severity of the risk to consumers and conferred standing.[103]

Conversely, when confronted with breaches involving more benign forms of data, courts have shown reluctance to infer a substantial risk of harm. For example, in *Beck v. McDonald*, the Fourth Circuit declined to confer standing after a laptop computer from a medical facility was either misplaced or stolen.[104] The laptop contained the personal information of approximately 7,400 patients, including "names, birth dates, the

---

[99] 848 F.3d 262, 274 (4th Cir. 2017).

[100] *Id.* at 275.

[101] *Id.*

[102] *See, e.g.*, Chambliss v. Carefirst, Inc., 189 F. Supp. 3d 564, 571 (D. Md. 2016) (collecting cases in which standing was conferred and noting that they consistently "either concerned *information more easily used in fraudulent transactions* or relied on factual allegations that the hackers had already misused the stolen data" (emphasis added)).

[103] *See, e.g.*, Attias v. Carefirst, Inc., 865 F.3d 620, 622–23 (D.C. Cir. 2017) (accepting as true at the pleading stage plaintiff's contention that social security and credit card numbers were stolen, despite defendant's contention that they were not); Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 690 (7th Cir. 2015) (malware compromising 350,000 customer credit cards); Krottner v. Starbucks Corp., 628 F.3d 1139, 1140, 1143 (9th Cir. 2010) (stolen laptop containing the social security numbers of 97,000 Starbucks employees).

[104] *Beck*, 848 F.3d at 267.

last four digits of social security numbers, and physical descriptors (age, race, gender, height, and weight)."[105] Despite the volume of data stolen, the lack of full social security numbers, credit card numbers, or bank account information on the laptop would make it difficult for a malicious hacker to successfully steal consumers' identities.[106]

3. Offers of Free Credit Monitoring Services

In an effort to aid consumers in protecting themselves from identity theft following a breach, some companies choose to offer free credit monitoring services to affected consumers.[107] Courts have interpreted such offers in two different ways. The first interpretation is that an offer to pay for credit monitoring is an admission of sorts by the company that the risk to consumers is substantial enough to necessitate protection.[108] In *Remijas*, the court explained "[i]t is telling . . . that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all [potentially affected] customers . . . . It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded."[109] Similarly, the Sixth Circuit in *Galaria v. Nationwide Mut. Ins. Co.* conferred standing, specifically noting that the defendant's offer of credit monitoring and identity-theft protection for one year was evidence that the company believed the risk to be substantial.[110]

---

[105] *Id.* Contrary to the medical center's policies and procedures, the laptop used to store the patients' information was unencrypted. After being notified of the breach, the plaintiffs—veterans who had received treatment at the facility—began "frequently monitor[ing] their credit reports, bank statements, health insurance reports, and other similar information, purchas[ed] credit watch services, and shift[ed] financial accounts." *Id.* (citation and internal quotation marks omitted). They consequently brought a class action suit, alleging that the defendant's failure to follow encryption policies caused them "embarrassment, inconvenience, unfairness, mental distress, and the threat of current and future substantial harm from identity theft and other misuse of their [p]ersonal [i]nformation." *Id.*

[106] *See* discussion *supra* Part I.B*; see also Beck*, 848 F.3d at 267 (indicating that only the last four digits of social security numbers were contained on the stolen laptop); *id.* at 274 n.6 (describing a single plaintiff who had experienced fraudulent charges on her credit card, but explaining that she could not attribute those charges to the breach in *Beck* given that there was no credit card information on the stolen laptop).

[107] Sarah Schaut, *What to Do After a Data Breach*, CREDIT KARMA (Dec. 4, 2018), https://www.creditkarma.com/id-theft/i/what-to-do-after-data-breach/.

[108] *See, e.g.*, *Remijas*, 794 F.3d at 694.

[109] *Id.*

[110] 663 F. App'x 384, 388 (6th Cir. 2016). The Sixth Circuit found Article III standing where hackers stole the personal information of 1.1 million of Nationwide's

The second, opposing interpretation is that it would be contrary to public policy to penalize companies for their decision to come to the aid of their customers.[111] For example, the court in *Beck* expressly opposed the presumption that the willingness of a defendant to pay for credit monitoring or identity theft services is an indicator of the likelihood of future injury.[112] The Fourth Circuit stated, "[c]ontrary to some of our sister circuits, we decline to infer a substantial risk of harm of future identity theft from an organization's offer to provide free credit monitoring services to affected individuals."[113] The court explained, as a policy matter, that "[t]o adopt such a presumption would surely discourage organizations from offering these services to data-breach victims, lest their extension of goodwill render them subject to suit."[114]

4. Mitigation Costs

In many cases, plaintiffs contend that they have already experienced actual harm, despite the absence of any attempted misuse of their personal data.[115] They argue instead that they have standing based on the time and money they have spent to protect themselves from possible identity theft.[116] Such plaintiffs seek recovery for claimed injuries such as time spent reviewing the breach, time spent monitoring their account information,

---

customers by breaking into its computer network. *Id.* at 385–86. In holding that there was a substantial risk of harm, the court pointed to Nationwide's offer of credit monitoring and identity-theft protection for one year, stating "[i]ndeed, Nationwide seems to recognize the severity of the risk." *Id.* at 388. It is unclear, however, how much the court relied on this fact in its finding of substantial risk. Notably, the court's finding was also predicated on general statistics of increased likelihood of harm, which are not typically accepted by other courts. *Id.* at 386. Furthermore, it is possible that the court may have been swayed by additional allegations included in a proposed amended complaint—that three unauthorized attempts had been made to open accounts in the plaintiff's name. *Id.* at 389 n.1.

[111] *See, e.g.*, *Beck*, 848 F.3d at 276.

[112] *Id.*

[113] *Id.*

[114] *Id.* The Third Circuit in *In re Horizon Healthcare Servs. Data Breach Litigation* agreed, holding that a company's offer "should not be used against it as a concession or recognition that the Plaintiffs have suffered injury," and sharing the concern that "such a rule would 'disincentivize[] companies'" from making gestures of good faith in the wake of a breach. 846 F.3d 625, 634 n.12 (3d Cir. 2017) (alteration in original).

[115] *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011) ("Appellants contend that an increased risk of identity theft is itself a harm sufficient to confer standing.").

[116] *See, e.g.*, *id.* at 44.

payments toward outside credit monitoring services, and the burden and expense of replacing credit cards.[117] The Supreme Court has held, however, that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[118] The lower court in *Clapper* had allowed standing when mitigation costs were prompted by a fear of future injury that was not " 'fanciful, paranoid, or otherwise unreasonable.' "[119] The Supreme Court expressly disagreed, explaining that such a standard would "water[] down" fundamental Article III standing requirements.[120] Courts before and after the *Clapper* decision have mirrored the same principle—that standing may not be premised on costs willingly incurred to protect against a perceived threat of identity theft.[121]

In the event of a breach, there is little that a breached company can offer outside of monetary damages. An injunction would not serve to protect the consumer from future harm because the company is powerless to reclaim the stolen data or otherwise curtail its use. The only adequate remedy would be to compensate the consumer for existing or certainly impending monetary damage inflicted upon him or her, rather than self-inflicted damage.

III. RECOMMENDATION

Evaluating constitutional standing in the context of data breach litigation presents a unique set of competing policy concerns. On one hand, consumers should have some avenue of redress when their data is stolen through no fault of their own. On the other, companies that fall victim to a breach are just

---

[117] *See, e.g.*, Krottner v. Starbucks Corp., 628 F.3d 1139, 1141 (9th Cir. 2010).

[118] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 416 (2013) (citing Pennsylvania v. New Jersey, 426 U.S. 660, 664 (1976) (per curiam); Nat'l Family Planning & Reprod. Health Ass'n, Inc. v. Gonzales, 468 F.3d 826, 831 (D.C. Cir. 2006)).

[119] *Clapper*, 568 U.S. at 416 (quoting Amnesty Int'l USA v. Clapper, 638 F.3d 118, 134 (2d Cir. 2011)).

[120] *Id.*

[121] *See, e.g.*, Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 694 (7th Cir. 2015) ("Mitigation expenses do not qualify as actual injuries where the harm is not imminent."); Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011) (quoting Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 8 (D.C. Cir. 2007)) ("That a plaintiff has willingly incurred costs to protect against an alleged increased risk of identity theft is not enough to demonstrate a 'concrete and particularized' or 'actual or imminent' injury."); Beck v. McDonald, 848 F.3d 262, 276–77 (4th Cir. 2017) ("Simply put, these self-imposed harms cannot confer standing.").

that—victims. It may not be fair to hold a breached company accountable for actions that were taken by third-party hackers. Breached companies often suffer their own harm in the wake of breach, in that they can lose the trust—and sometimes the business—of many of their customers.[122] With the ever-increasing sophistication of hackers, it is also possible for companies to suffer a breach despite making every good faith effort to protect their systems.[123] Fairness to affected consumers must therefore be balanced against fairness to the companies experiencing a breach.

Neither case law nor current legislation provides a bright line rule as to which factual scenarios should result in standing for the consumers impacted by a breach. The precedent that does exist to date is inconsistent in several areas. Due to the wide array of factual circumstances that can surround a breach, with regard to the extent, method, and intent behind the breach, the size, industry, and precautions taken by the breached company, and information known about injury to other consumers, a bright line rule may not be feasible or appropriate. The remainder of this Note will discuss the goals that should guide the formulation of an effective method for analyzing standing in data breach cases, suggesting one possible solution that seeks to achieve these goals.

A. Balancing Competing Interests

The most important objective of any proposed solution to address consumer standing is to balance the interests of the consumer against the interests of the breached company. An effective solution would recognize that companies are rarely the culpable party behind a hack, and that consumers typically bring suit against the breached company because they are unable to identify and seek recovery from the true offender—the hacker. Fairness demands a flexible solution that will protect consumers

---

[122] *See* Herb Weisbaum, *The Total Cost of a Data Breach—Including Lost Business—Keeps Growing*, NBC NEWS (July 30, 2018, 3:15 PM), https://www.nbcnews.com/business/consumer/total-cost-data-breach-including-lost-business-keeps-growing-n895826 (citing *2018 Cost of a Data Breach Study: Global Overview*, IBM SECURITY 1, 7 (July 2018), https://www.ibm.com/ downloads/cas/861MNWN2).

[123] *See* Herb Weisbaum, *Cyber Threats are 'Mind Blowing,' Crooks Getting Smarter: Report*, NBC NEWS (Apr. 12, 2016, 8:54 AM), https://www.nbcnews.com/mach/features/cyber-threats-are-mind-blowing-crooks-getting-smarter-report-n554176 (discussing the increasing sophistication of hackers and indicating that "[c]riminal hackers don't give up when their attack is unsuccessful").

who entrusted their personal information to a company in good faith and who are now vulnerable as a result. At the same time, companies who have made reasonable efforts to secure the data in their care, and are essentially victims of a hack, should be protected as well.

An appropriate framework for evaluating standing would aim to encourage companies to be proactive about securing the data in their possession. Punishing companies that have done everything in their power to prevent a breach by subjecting them to litigation would disincentivize such socially desirable action in the future. Ideally, a company should be able to insulate itself from liability by making good faith efforts to invest in data security for the benefit of its customers. Companies that do not make a good faith effort to protect their systems, on the other hand, should be held accountable for their inaction.

In determining what constitutes good faith action, courts must recognize that a company's ability to implement and monitor systems to protect against breaches is dependent on, and often limited by, its financial resources. A small company cannot reasonably be expected to implement the same security measures as a large institution worth billions of dollars.[124] Moreover, the degree of protection necessary should increase with the sensitivity of the data that the company possesses. Companies charged with safeguarding social security numbers and other personally identifiable information[125] that could enable hackers to open unauthorized accounts in customers' names should be held to the highest standard, since customers stand to lose the most from a breach of such information. Likewise, companies in possession of customers' credit card information should be held to a high standard, given the ease with which hackers can misuse such data.[126] A lower standard should then apply to companies holding data that is unlikely to be pursued or misused by hackers—for example, telephone numbers. Because the degree and sophistication of breaches is continually evolving, companies and courts alike should expect such standards to evolve accordingly.

---

[124] *See generally* Loren F. Selznick & Carolyn LaMacchia, *Cybersecurity Liability: How Technically Savvy Can We Expect Small Business Owners To Be?*, 13 J. BUS. & TECH. L. 217 (2018).

[125] *See supra* note 44 and accompanying text.

[126] *See* discussion *supra* Part I.B.

An effective solution to the determination of standing should also consider the position of both parties with respect to discovery. As previously discussed, a plaintiff must allege injury-in-fact, causation, and redressability at the pleadings stage in order to establish standing. Setting a standard that would make it easier for plaintiffs to meet these requirements would enable them to further build their case with the benefit of full-fledged discovery. It may also, however, allow cases to reach the discovery phase, only to find that insufficient evidence exists for the case to survive. While this trade-off may be beneficial to consumers, forcing every breached company to undergo extensive discovery would significantly burden both company resources and the judicial system. By the same logic, a standard that would limit the quantity of cases reaching the discovery phase would benefit companies and promote judicial economy, but may prevent many consumers from pursuing the recovery they rightfully deserve. An effective solution would thus enable consumers to obtain the information they need to figure out whether or not they can—and should—bring suit, without unduly burdening breached companies.

B. Proposed Quadrant Framework for Judicial Analysis

A potential solution to the issue of standing in data breach cases is to allow consumers whose data has been accessed in a breach to conduct a limited form of discovery in order to determine whether their risk of harm is sufficiently imminent to confer standing.[127] The scope of such discovery would be limited to address the sole question of whether the necessary evidence exists to "push [a] threatened injury of future identity theft beyond the speculative to the sufficiently imminent."[128] In order to minimize the burden and obstacles placed on both plaintiffs and defendants in gathering the information necessary to

---

[127] As it currently stands:

> A plaintiff has no right to discovery in opposing a motion to dismiss for lack of standing . . . , since [such] a motion . . . involves an examination of the face of the complaint, which does not depend upon discovery. In considering standing . . . , only the court, not the plaintiff (or defendant), can elicit information outside the pleadings.

Motions To Dismiss, 7 Cyc. of Federal Proc. § 25:11 (3d ed.). The proposed framework would establish a middle ground between this current no-discovery rule and full discovery, enabling both parties to request information from the other pertinent only to standing.

[128] Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017).

evaluate the sole question of standing, the proposed limited discovery would consist of a standardized form to be completed by the breached company and plaintiff.[129] This would also lessen the burden on attorneys and judges by avoiding the full discovery process associated with litigation, including drafting case-specific requests, creating discovery schedule, and managing discovery deadlines.[130]

The form itself, which could be made available on a public website or be forwarded by the company as part of data breach notification requirements, would collect information about the company itself, the specific breach, and the company's systems and history of breaches. Regarding the company itself, pertinent data would include the industry, the volume of consumer data entrusted to the company, and the existence of any warranties concerning data security that may give rise to a contractual claim by consumers. Regarding the particular breach in question, the survey would ask how many consumers were impacted, what kind of data was stolen—in the form of "check all that apply"—and was the stolen data encrypted?

With respect to security systems, companies would be asked to describe the security measures currently in place to protect against a data breach, and to detail how much the company has paid to date to implement and maintain its current data security scheme. Such an accounting would include, for example, the initial cost of installation of any programs, annual maintenance costs, and labor or outside services costs associated with maintaining and monitoring data security. While this may seem like a lot of information to ask of a company, consider that a company need only collect the information once. It could then resubmit the same portion of the form for any subsequent breaches that may occur, merely adjusting for any system updates made since the last breach.

Lastly, with respect to a company's history of breaches, it would be asked whether any other breaches had occurred over the past five years and, if so, to provide the dates of each and the

---

[129] The benefit of precluding discovery before a court's subject matter jurisdiction—including standing—has been established is that it "protects both plaintiff and defendant from burdensome and unnecessary discovery at a premature stage of the proceedings." *Motions to Dismiss*, 7 Cyc. of Federal Proc. § 25:11 (3d ed.). The goal of a standardized form designed to address standing inquiries is to open the door to discovery just far enough to avoid a heavy burden.

[130] *See* FED. R. CIV. P. 26(f) (Conference of the Parties; Planning for Discovery); FED. R. CIV. P. 16(b) (Scheduling Orders).

number of consumers impacted. The purpose here would be to determine if a substantially similar breach has occurred—that is, one involving the same defendant, timing, and security measures, or lack thereof—and to gauge the company's response. In other words, did the company implement any upgrades or alterations to mitigate system vulnerability? After obtaining responses from the breached company, consumer plaintiffs would submit the results of limited discovery to the court, along with information about their experience—specifically, the existence of any offer by the company to provide credit monitoring and the amount of mitigation costs expended by all parties.

After the information is submitted, the court must confront the dilemma of evaluating the substantiality of the risk to consumers. Under the proposed framework, a court would conduct a balancing test between the magnitude and likelihood of harm to the consumer and the precautions taken by the breached company—does it make sense to hold the company liable above and beyond what it has already paid to prevent such an occurrence? The balancing test can be likened to the famous "Hand Formula" for determining liability in a negligence action: B=PL, where B=burden, or the investment in precaution, P=probability of harm, and L=loss, or the magnitude of harm.[131] According to the formula, liability—or in this situation, standing—"depends on whether B is less than L multiplied by P."[132] Put another way, individual data breach cases can be broken up into four quadrants, similar to the well-known impact/effort matrix used to prioritize tasks,[133] but with the consumer's likely harm (PL) on one axis and the company's

---

[131] *See* United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947).

[132] *Id.*

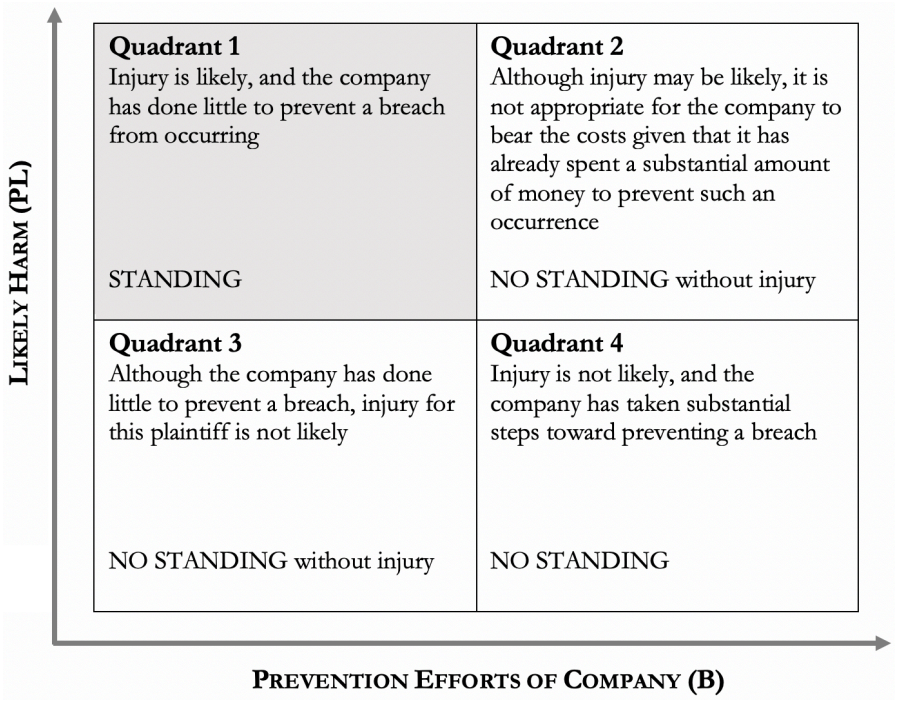
> Though mathematical in form, the Hand formula does not yield mathematically precise results in practice; that would require that B, P, and L all be quantified, which so far as we know has never been done in an actual lawsuit. Nevertheless, the formula is a valuable aid to clear thinking about the [relevant] factors . . . and about the relationship among those factors.

U.S. Fid. & Guar. Co. v. Plovidba, 683 F.2d 1022, 1026 (7th Cir. 1982).

[133] *See* Allen Graves, *Effort/Impact Matrix*, SIX SIGMA DAILY (Jan. 4, 2013), https://www.sixsigmadaily.com/effort-impact-matrix/. The matrix involves plotting potential actions on a chart with effort on one axis and impact on the other. This allows for the identification of so-called low hanging fruit, "which of the numerous solutions to implement appear to be the easiest (least effort) while having the most favorable impact." *Id.* Those tasks or solutions in the quadrant of low-effort, high-impact are implemented first.

prevention efforts (B) on the other, as illustrated in Figure 1 below. Applying such a concept in this context puts emphasis on the standing prongs of both injury-in-fact and causation.

FIGURE 1: FACTUAL QUADRANT MODEL FOR CONSUMER STANDING



In the absence of evidence of actual injury by the plaintiff, standing would be found only in the first quadrant. The issue then becomes how to determine which quadrant a particular case falls into. As a purely mathematical formula is impractical, the court would consider certain factors to determine where along the spectrum of each axis a case would fall.

Along the injury axis, the type of data compromised is a critical factor to consider. Full social security numbers and credit card numbers—especially both—would increase the risk and magnitude of harm to consumers, since these forms of data can easily be used to effectuate identity theft. The last four digits of social security numbers or credit card numbers, or encrypted data, by contrast, would not hold as much weight. Another factor to consider would be the harm to others impacted by the same breach. Since many breaches result in no identity

theft or fraudulent charges, the presence of another consumer who suffered actual injury speaks to the malicious intent of the hackers and, thus, the probability that they will engage in further malicious behavior. While courts have expressed disapproval of the use of general statistics,[134] limiting the analysis to the statistics of the same breach addresses this concern.

Along the burden axis, the effort and cost associated with a company's current security measures are the clearest indicator of the burden on the company. This must be evaluated in light of the type of industry in which the company operates and the volume and types of customer data it safeguards. The goal here is to incentivize companies to expend an appropriate amount on precautionary measures to protect their customers from breaches and to protect themselves from future litigation. A company would have the ability, by making the necessary efforts toward preventing a breach, to place itself squarely in the two quadrants—two and four above[135]—where it could never be subject to suit in the absence of actual injury, in the form of identity theft or fraudulent charges. A company's offer to pay for credit monitoring would also be taken into account—not as an indicator of the likelihood of harm—but as evidence of the company's attempt to take some of the burden off of consumers. If a company had experienced data breaches in the past, its response—namely, whether it made changes to its systems to avoid recurrence—would speak to its accountability for future breaches.

CONCLUSION

"[N]ow more than ever it's important for organizations of all sizes to not only be prepared for a data breach, but to also be taking proactive steps to plan for the inevitability."[136] In light of the ever-increasing prevalence of data breaches, it is critical to identify a consistent method for analyzing risk for purposes of

---

[134] The *Beck* court, for example, rejected the idea that a "substantial risk" of harm could be inferred through statistics—for example, that data breach victims are 9.5 times more likely to suffer identity theft and that 19% of data breach victims become victims of identity theft—explaining that a general statistic fails to address "the risk arising out of any particular incident, nor does it address the particular facts of this case." Beck v. McDonald, 848 F.3d 262, 275 n.7 (4th Cir. 2017).

[135] *See supra* Figure 1.

[136] *ITRC Data Breach Report*, *supra* note 10, at 3 (quoting Matt Cullina, CEO of CyberScout).

standing. Not only should consumers be aided in their decisions whether or not to file suit, but companies should be able to rely on the predictability of the courts' decision-making in order to properly shield themselves from litigation. The methodology discussed above represents a starting point for such evaluation. It would also have the added benefit of creating a standard method of data collection to improve our understanding of which factors in a data breach most often lead to identity theft or fraudulent charges to consumers.